					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII10					Tytuł dokumentu: **Polityka retencji, usuwania i utylizacji PII**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma / regulacja	Klauzula / środek kontrolny / artykuł	Zastosowanie	Typ pokrycia	Komentarz
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Udokumentowane dowody retencji i kontrola operacyjna
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorowanie, niezgodności i działania korygujące
ISO/IEC 27701:2025	Annex A.1.2.8; Annex A.1.2.9	Controller / Joint Controller	Supporting	Wspólna odpowiedzialność i rejestry przetwarzania
ISO/IEC 27701:2025	Annex A.1.3.7; Annex A.1.3.8	Controller	Supporting	Wsparcie wykonania usunięcia
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Retencja, usuwanie i utylizacja
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Polecenia klienta i rejestry podmiotu przetwarzającego
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3	Processor	Primary	Wsparcie usuwania i zdolność do utylizacji
ISO/IEC 27701:2025	Annex A.3.20; Annex A.3.21; Annex A.3.24	Both	Supporting	Utylizacja nośników i postępowanie z kopiami zapasowymi
GDPR	Article 5(1)(e); Article 5(2)	Controller	Primary	Ograniczenie przechowywania i rozliczalność
GDPR	Article 17	Controller	Supporting	Wsparcie wykonania usunięcia
GDPR	Article 24	Controller	Supporting	Środki administratora
GDPR	Article 26	Joint Controller	Supporting	Podział wspólnej odpowiedzialności
GDPR	Article 28	Processor	Supporting	Usuwanie i zwrot przez podmiot przetwarzający

GDPR	Article 30	Both	Supporting	Rejestry przetwarzania
GDPR	Article 32	Both	Supporting	Bezpieczne przetwarzanie i wsparcie utylizacji
ISO/IEC 29100:2020	Clause 5.5; Clause 5.6; Clause 5.10	Both	Supporting	Minimalizacja, ograniczenie retencji i rozliczalność
ISO/IEC 29151:2022	Annex A.7; Annex A.7.2	Both	Supporting	Środki kontroli retencji i usuwania plików tymczasowych
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Both	Primary	Ramy usuwania i dokumentacja
ISO/IEC 27555:2025	Clause 7.2; Clause 7.3; Clause 8.3	Controller	Primary	Okresy usuwania i reguły usuwania
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Both	Primary	Wdrożenie i wyjątki
ISO/IEC 27555:2025	Clause 10.1; Clause 10.2; Clause 10.3	Both	Primary	Odpowiedzialności i nadzór nad wdrożeniem
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integracja ryzyka dla prywatności
ISO/IEC 27002:2022	Control 7.14; Control 8.10	Both	Supporting	Bezpieczna utylizacja i usuwanie informacji

1. Zakres

1.1 Niniejsza polityka ustanawia wymagania organizacji dotyczące definiowania, przeglądu, wykonywania i dokumentowania dowodami retencji, usuwania, anonimizacji, deidentyfikacji, zwrotu, transferu i utylizacji PII.

1.2 Niniejsza polityka ma zastosowanie do PII przetwarzanych w kontekstach administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania, w tym PII przechowywanych w systemach produkcyjnych, archiwach, kopiach zapasowych, replikach, logach, środowiskach testowych, plikach tymczasowych, dokumentacji papierowej i nośnikach pamięci.

1.3 Niniejsza polityka ma zastosowanie do obowiązków dotyczących retencji i usuwania wynikających z zatwierdzonych celów przetwarzania, zapisów podstaw prawnych, poleceń administratora, wymogów umownych, wyników realizacji usunięcia na rzecz osób, których dane dotyczą, zakończenia usługi, utylizacji nośników pamięci oraz ustaleń z monitorowania PIMS.

1.4 Niniejsza polityka nie określa wyboru podstawy prawnej, treści klauzuli informacyjnej, pełnej obsługi praw osób, których dane dotyczą, nadzoru nad cyklem życia podmiotu przetwarzającego, mechanizmów transferu międzynarodowego, architektury środków bezpieczeństwa, procesu reagowania na incydenty ani metodyki audytu PIMS. Te środki kontroli są ujęte w powiązanych politykach.

1.5 Na potrzeby niniejszej polityki istotna zmiana oznacza każdą zmianę celu przetwarzania, kategorii PII, kategorii osoby, której dane dotyczą, lokalizacji przechowywania w systemie, przepisów lub umowy dotyczących retencji, polecenia klienta, architektury kopii zapasowych, podejścia do archiwizacji, metody utylizacji, ustaleń z podmiotem przetwarzającym lub podwykonawcą przetwarzania, procesu usuwania albo zakresu certyfikacji PIMS, która wpływa na retencję, usuwanie lub utylizację.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, że PII są przechowywane wyłącznie w zatwierdzonych celach i okresach, usuwane lub w inny sposób utylizowane, gdy nie są już wymagane, oraz poparte dowodami gotowymi do audytu.

2.2 Niniejsza polityka umożliwia organizacji wykazanie ograniczenia przechowywania, rozliczalnego nadzoru nad retencją, kontrolowanego wykonania usuwania, bezpiecznej utylizacji, zgodności z poleceniami dla podmiotów przetwarzających, kontroli wyjątków oraz ciągłego doskonalenia bez tworzenia odrębnego rejestru usuwania.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 określenie właścicielstwa reguł retencji oraz wymaganych metadanych retencji;

3.1.2 zapewnienie, że reguły retencji są odnotowywane w inwentarzu przetwarzania PII / ROPA;

3.1.3 zapewnienie, że działania podmiotu przetwarzającego i podwykonawcy przetwarzania dotyczące usuwania opierają się na poleceniu klienta lub umowie;

3.1.4 zapewnienie, że PII po upływie okresu przechowywania są usuwane, zwracane, transferowane, anonimizowane, deidentyfikowane lub utylizowane z użyciem zatwierdzonych metod;

3.1.5 rozróżnienie systemów produkcyjnych, archiwów, kopii zapasowych, replik, logów, obszarów testowych i plików tymczasowych;

3.1.6 zapewnienie, że dowody usuwania i utylizacji są przechowywane w kanonicznych obiektach dowodowych PIMS;

3.1.7 zapewnienie, że wyjątki dotyczące retencji są ograniczone czasowo, zatwierdzone i poddawane przeglądowi;

3.1.8 zintegrowanie monitorowania retencji i usuwania z niezgodnościami, działaniami korygującymi i doskonaleniem.

4. Postanowienia polityki

4.1 Przypisanie reguły retencji

4.1.1 [Controller] Process Owner / Business Owner MUST przypisać udokumentowaną regułę retencji do każdej czynności przetwarzania administratora w REG02 przed rozpoczęciem tej czynności przetwarzania.

4.1.2 [Joint Controller] Process Owner / Business Owner MUST odnotować podział odpowiedzialności współadministratorów za retencję i usuwanie w REG02 i REG08 przed rozpoczęciem lub zmianą wspólnego przetwarzania.

4.1.3 [Processor] Vendor / Procurement Owner MUST odnotować polecenia klienta dotyczące retencji, zwrotu, transferu lub usuwania dla działań podmiotu przetwarzającego w REG08 przed rozpoczęciem lub zmianą przetwarzania przez podmiot przetwarzający.

4.1.4 [Subprocessor] Vendor / Procurement Owner MUST odnotować wymagania przeniesione na podwykonawcę przetwarzania dotyczące retencji, zwrotu, transferu lub usuwania w REG08 przed onboardingiem podwykonawcy przetwarzania lub zmianą polecenia.

4.1.5 [Both] Privacy Lead / PIMS Manager MUST zweryfikować, że każda zatwierdzona reguła retencji w REG02 obejmuje okres przechowywania, zdarzenie rozpoczynające bieg okresu, właściciela, uzasadnienie, końcowy sposób postępowania z danymi i datę następnego przeglądu przed zatwierdzeniem reguły.

4.1.6 [Both] Data Protection Officer / Privacy Advisor MUST odnotować poradę w REG02 lub REG12 przed zatwierdzeniem każdej reguły retencji obejmującej konflikt prawny, przetwarzanie wysokiego ryzyka, PII szczególnej kategorii lub przechowywanie wykraczające poza pierwotny cel przetwarzania.

4.2 Przegląd i ograniczenie retencji

4.2.1 [Both] Process Owner / Business Owner MUST dokonywać przeglądu przypisanych reguł retencji w REG02 co najmniej raz w roku oraz w ciągu 30 dni od istotnej zmiany.

4.2.2 [Both] Privacy Lead / PIMS Manager MUST zatwierdzić albo odrzucić nowe lub zmienione reguły retencji w REG02 w ciągu 10 dni roboczych od ich przedłożenia.

4.2.3 [Both] System Owner / Application Owner MUST potwierdzić techniczną lub ręczną metodę egzekwowania każdej reguły retencji w REG02 przed uruchomieniem produkcyjnym oraz podczas każdego rocznego przeglądu retencji.

4.2.4 [Controller] Process Owner / Business Owner MUST ograniczyć aktywne wykorzystywanie PII przechowywanych wyłącznie z przyczyn prawnych, umownych, audytowych lub spornych w REG02 w ciągu pięciu dni roboczych od zidentyfikowania przesłanki ograniczenia.

4.2.5 [Both] Privacy Lead / PIMS Manager MUST odnotować nierozwiązane ryzyko nadmiernego przechowywania lub zaległy przegląd retencji w REG12 w ciągu pięciu dni roboczych od identyfikacji.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wyjątki

9.1.1 [All] Process Owner / Business Owner MUST przedłożyć każdy wniosek o przechowywanie PII wykraczające poza zatwierdzoną regułę retencji w REG02 w REG12, zanim wyjątek stanie się aktywny.

9.1.2 [All] Privacy Lead / PIMS Manager MUST zatwierdzić albo odrzucić wnioski o wyjątek dotyczący retencji w REG12, zanim wyjątek stanie się aktywny.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUST odnotować poradę w REG12 przed zatwierdzeniem każdego wyjątku obejmującego konflikt prawny, odmowę usunięcia, PII wysokiego ryzyka, udostępnianie zewnętrzne lub wpływ na certyfikację.

9.1.4 [All] Top Management MUST zatwierdzić wyjątki dotyczące retencji przekraczające 90 dni, wpływające na przetwarzanie wysokiego ryzyka lub wpływające na zewnętrzne zapewnienie w REG12, zanim wyjątek stanie się aktywny.

9.1.5 [All] Privacy Lead / PIMS Manager MUST przypisać właściciela, datę wygaśnięcia, środek kompensujący i częstotliwość przeglądu w REG12 dla każdego zatwierdzonego wyjątku dotyczącego retencji, usuwania lub utylizacji.

9.1.6 [All] Privacy Lead / PIMS Manager MUST dokonywać przeglądu każdego otwartego wyjątku w REG12 co najmniej raz w miesiącu do jego zamknięcia.

9.1.7 [All] Process Owner / Business Owner MUST zamknąć lub odnowić każdy wyjątek w REG12 przed datą wygaśnięcia wyjątku.

10. Egzekwowanie

10.1.1 [All] Privacy Lead / PIMS Manager MUST odnotować niezgodność w REG12 w ciągu pięciu dni roboczych od zidentyfikowania brakujących metadanych retencji, zaległego przeglądu retencji, nieuzasadnionego przechowywania, pominiętego działania końcowego sposobu postępowania z danymi lub brakujących dowodów.

10.1.2 [All] System Owner / Application Owner MUST wstrzymać nowe użycie produkcyjne czynności przetwarzania w REG12, gdy wymagane techniczne środki kontroli retencji nie istnieją przed uruchomieniem produkcyjnym.

10.1.3 [All] Process Owner / Business Owner MUST wstrzymać niezatwierdzone aktywne wykorzystywanie PII przechowywanych wyłącznie z przyczyn prawnych, umownych, audytowych lub spornych w ciągu pięciu dni roboczych i odnotować działanie w REG02 lub REG12.

10.1.4 [Processor] Vendor / Procurement Owner MUST eskalować zaległe działania końcowego sposobu postępowania z danymi wykonywane na polecenie klienta w REG08 i REG12 w ciągu pięciu dni roboczych od niedotrzymania terminu umownego.

10.1.5 [Subprocessor] Vendor / Procurement Owner MUST eskalować brakujące dowody końcowego sposobu postępowania z danymi przez podwykonawcę przetwarzania w REG08 i REG12 w ciągu pięciu dni roboczych od niedotrzymania umownego terminu dostarczenia dowodów.

10.1.6 [All] Internal Audit / Compliance Reviewer MUST zweryfikować skuteczność działań korygujących dla niezgodności dotyczących retencji, usuwania i utylizacji w REG12 podczas następnego zaplanowanego audytu albo w ciągu 60 dni od zamknięcia, w zależności od tego, co nastąpi wcześniej.

10.1.7 [Conditional] Incident Response Coordinator MUST zainicjować obsługę REG10, gdy niezgodność dotycząca retencji, usuwania lub utylizacji wskazuje na podejrzenie incydentu dotyczącego PII.

11. Przegląd i utrzymanie

11.1.1 [All] Privacy Lead / PIMS Manager MUST dokonywać przeglądu niniejszej polityki raz w roku i odnotowywać wynik przeglądu w REG12.

11.1.2 [All] Privacy Lead / PIMS Manager MUST dokonać przeglądu niniejszej polityki w ciągu 30 dni od istotnej zmiany przepisów dotyczących retencji, celu przetwarzania, polecenia dla

podmiotu przetwarzającego, architektury systemu, architektury kopii zapasowych, podejścia do archiwizacji, procesu usuwania, procesu utylizacji lub wymagań certyfikacji PIMS.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUST dokonać przeglądu istotnych dla prywatności zmian niniejszej polityki w REG12 przed zatwierdzeniem.

11.1.4 [All] Top Management MUST zatwierdzić istotne zmiany niniejszej polityki w REG12 przed publikacją.

11.1.5 [All] Privacy Lead / PIMS Manager MUST odnotować komunikację zatwierdzonych zmian polityki w REG11 w ciągu 30 dni od publikacji.

12. Powiązane polityki

12.1 Niniejszą politykę wspierają następujące powiązane polityki:

12.2 PII01 - Polityka systemu zarządzania informacjami o prywatności

12.3 PII02 - Polityka ról, odpowiedzialności i rozliczalności w zakresie prywatności

12.4 PII03 - Polityka inwentarza przetwarzania PII i podstaw prawnych

12.5 PII04 - Polityka klauzul informacyjnych i przejrzystości

12.6 PII06 - Polityka zarządzania prawami osób, których dane dotyczą

12.7 PII08 - Polityka privacy by design i privacy by default

12.8 PII09 - Polityka gromadzenia, wykorzystywania, ujawniania i udostępniania PII

12.9 PII12 - Polityka zarządzania prywatnością podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich

12.10 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.11 PII15 - Polityka zarządzania incydentami i naruszeniami dotyczącymi PII

12.12 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami PIMS

12.13 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS

13. Normy i ramy odniesienia

13.1 Niniejsza polityka jest zmapowana na następujące normy i regulacje. Mapowanie wyjaśnia, w jaki sposób polityka wspiera przywołane wymagania, oraz wskazuje wewnętrzne klauzule, które je wdrażają lub wspierają.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Zmapowano na udokumentowane dowody retencji, planowanie operacyjne, metadane retencji, dowody wdrożenia oraz zapisy wykonania cyklu życia. Addressed by clauses [4.1.5; 4.2.3; 4.3.5; 4.4.1; 7.1.1; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Zmapowano na monitorowanie, metryki, przegląd zaległych działań, niezgodności oraz działania korygujące dla środków kontroli retencji, usuwania i utylizacji. Addressed by clauses [4.2.5; 6.1.1; 6.1.2; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 10.1.1; 10.1.6].

13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Zmapowano na dowody odpowiedzialności współadministratorów oraz rejestry przetwarzania administratora zawierające metadane retencji i końcowego sposobu postępowania z danymi. Addressed by clauses [4.1.1; 4.1.2; 4.1.5; 4.2.1; 6.1.4; 7.1.2].

13.2.4 **Annex A.1.3.7; Annex A.1.3.8** - Zmapowano na wsparcie wykonania usunięcia, kierowanie oceny usunięcia oraz powiązanie dowodów stron trzecich, gdy wyniki usunięcia wymagają działania. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.2.5 **Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9** - Zmapowano na usunięcie lub deidentyfikację na koniec przetwarzania, postępowanie z plikami tymczasowymi, ograniczenie retencji oraz udokumentowane środki kontroli końcowego sposobu postępowania

z danymi. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.2.4; 4.3.1; 4.3.5; 4.3.6; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Zmapowano na umowy z klientami podmiotu przetwarzającego, udokumentowane cele klienta oraz rejestry przetwarzania podmiotu przetwarzającego. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7].

13.2.7 **Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3** - Zmapowano na wsparcie podmiotu przetwarzającego dla obowiązków klienta, postępowanie z plikami tymczasowymi oraz zdolność do zwrotu, transferu lub końcowego sposobu postępowania z danymi. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 10.1.4; 10.1.5].

13.2.8 **Annex A.3.20; Annex A.3.21; Annex A.3.24** - Zmapowano na postępowanie z cyklem życia nośników pamięci, kontrole ponownego użycia lub wydania sprzętu oraz postępowanie z kopiami zapasowymi dla PII. Addressed by clauses [4.3.6; 4.3.7; 4.4.1; 4.4.3; 4.4.4; 4.4.6; 5.1.4].

13.3 GDPR

13.3.1 **Article 5(1)(e); Article 5(2)** - Zmapowano na ograniczenie przechowywania, rozliczalność retencji, zatwierdzone metadane retencji, dowody i przegląd. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 4.2.4; 4.3.1; 4.3.5; 6.1.1; 8.1.1; 8.1.2; 10.1.1].

13.3.2 **Article 17** - Zmapowano na zatwierdzone kierowanie wyników usunięcia, dowody wykonania oraz eskalację incydentu, gdy nieskuteczność kontroli usuwania wskazuje na podejrzenie incydentu dotyczącego PII. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.3.3 **Article 24** - Zmapowano na nadzór administratora, środki rozliczalności, przeglądy, wyjątki, działania korygujące i utrzymanie polityki. Addressed by clauses [4.1.6; 6.1.2; 6.1.3; 9.1.2; 9.1.3; 9.1.4; 11.1.1; 11.1.2; 11.1.4].

13.3.4 **Article 26** - Zmapowano na podział odpowiedzialności współadministratorów za retencję i usuwanie. Addressed by clauses [4.1.2; 6.1.4].

13.3.5 **Article 28** - Zmapowano na zgodność z poleceniami dla podmiotów przetwarzających i podwykonawców przetwarzania, zwrot, transfer, końcowy sposób postępowania z danymi, dowody i eskalację. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7; 10.1.4; 10.1.5].

13.3.6 **Article 30** - Zmapowano na metadane retencji i końcowego sposobu postępowania z danymi w rejestrach przetwarzania dla czynności administratora i podmiotu przetwarzającego. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.2.1; 4.4.1; 7.1.2].

13.3.7 **Article 32** - Zmapowano na bezpieczną operacyjną obsługę przechowywanych PII, egzekwowanie techniczne, kontrolę nośników pamięci, postępowanie z kopiami zapasowymi i eskalację incydentów. Addressed by clauses [4.2.3; 4.3.6; 4.4.3; 4.4.4; 4.4.6; 7.1.3; 7.1.4; 7.1.8].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.5; Clause 5.6; Clause 5.10** - Zmapowano na minimalizację danych, ograniczenie wykorzystywania i retencji, końcowy sposób postępowania z danymi, gdy dane nie są już wymagane, ograniczenie przechowywanych PII oraz dowody rozliczalności. Addressed by clauses [4.1.5; 4.2.1; 4.2.4; 4.3.1; 4.4.2; 4.5.1; 4.5.2; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.7; Annex A.7.2** - Zmapowano na ograniczoną czasowo retencję, końcowy sposób postępowania z danymi, zautomatyzowane lub ręczne egzekwowanie oraz

postępowanie z plikami tymczasowymi. Addressed by clauses [4.2.3; 4.3.1; 4.4.5; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.6 ISO/IEC 27555:2025

13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8** - Zmapowano na nadzór nad ramami usuwania, grupowanie PII, okresy retencji i usuwania, rozróżnienie archiwów i kopii zapasowych, strukturę reguł usuwania oraz wymagania dotyczące udokumentowanej procedury. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 7.1.1; 7.1.2].

13.6.2 **Clause 7.2; Clause 7.3; Clause 8.3** - Zmapowano na określenie regularnych okresów usuwania, identyfikację standardowego okresu usuwania oraz przypisanie reguł usuwania do czynności przetwarzania PII. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 7.1.1; 7.1.2].

13.6.3 **Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7** - Zmapowano na wymagania wdrożeniowe dla systemów, procesów ręcznych, aspektów ogólnoorganizacyjnych, podmiotów przetwarzających, obsługi odzyskiwania oraz zarządzania wyjątkami. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 9.1.1; 9.1.5; 9.1.6].

13.6.4 **Clause 10.1; Clause 10.2; Clause 10.3** - Zmapowano na przypisanie ról, dokumentację, osadzenie operacyjne, audyt i nadzór nad wdrożeniem retencji, usuwania i utylizacji. Addressed by clauses [5.1.2; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.9; 6.1.7; 7.1.3; 7.1.4; 11.1.1; 11.1.2].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Zmapowano na oparty na ryzyku nadzór nad prywatnością, świadomość kierownictwa, integrację ryzyka dla prywatności z PIMS oraz kontekst ryzyka związanego z retencją. Addressed by clauses [4.1.6; 4.2.5; 4.5.4; 6.1.2; 6.1.3; 9.1.3; 9.1.4].

13.8 ISO/IEC 27002:2022

13.8.1 Control 7.14; Control 8.10 - Zmapowano na usuwanie informacji, kontrolowane zakończenie cyklu życia, wydanie nośników pamięci oraz dowody końcowego sposobu postępowania z danymi. Addressed by clauses [4.3.1; 4.3.5; 4.3.6; 4.3.7; 4.4.4; 4.4.5; 7.1.3; 7.1.4; 10.1.2].